

# Safer learning with Google for Education

Enable students to learn in a safer digital environment free from ads, spam, or cyberthreats. Provide the same enterprise-grade security that protects the data of billions who use Google products every day – without administrative burden.

Google Workspace for Education and Chromebook products are secure by default, private by design, and put schools in control.



## How does Google for Education protect school data?

All Google products are secure by default and continuously protected by end-to-end processes that automatically detect and prevent online threats. Tools similar to those that [block 99.9% of spam emails in Gmail – over 100 million each day](#) – keep sensitive data safe and support compliance with major international security and privacy standards.

Google encrypts data and protects it with multiple layers of security. Google [data centers](#) use Google-designed hardware and systems optimized for security and performance. The result? Data is secured at every point, which enables us to recognize, respond, and rapidly remediate threats. In fact, Google Workspace is one of the [world's most secure](#) cloud-native communication and collaboration suites; and there have been zero reported successful ransomware attacks on Chromebooks.

## Does Google use data from schools?

### Schools own their data

Schools retain full rights over the intellectual property their users put into Google Workspace for Education and can set rules and permissions for how and when someone in their school community can access or download data or documents. Google does not own, use, or sell any customer data contained in [Google Workspace for Education Core Services](#). We protect this data with strict security protocols and provide full transparency and comprehensive privacy policies with strict security protocols.

### Transparency schools can trust

Google is committed to transparency regarding data collection policies and practices. The [Google Workspace for Education Privacy Notice](#) and [Google Workspace Terms of Service](#) explain our commitments to protect data.

### No ads in Google Workspace for Education Core Services

We don't use or sell Google Workspace for Education customer data to third parties, and we do not share data placed in our systems with third parties, unless specifically requested by the data owner, under circumstances described in the [Google Workspace for Education Privacy Notice](#), or as required by law.

## Can I use Google Workspace for Education in compliance with legal standards?

Google supports compliance with rigorous security and privacy standards, including FERPA, COPPA, and GDPR, and we're audited by independent [third-party](#) organizations. For a complete list of global compliance standards, [visit our Cloud Compliance & Regulations Resources center](#).

## Can admins manage and secure school domains?

We make it easy for administrators to maintain domains with tools to help monitor and manage data security, offer enhanced control, and increase visibility. Built-in, automated protections provide 24/7 monitoring, data encryption, data loss prevention (DLP), identity and access management, and much more.

Administrators have centralized controls in the [Admin console](#) for privacy, security, data, and device management. From there, the [security center](#) provides automatic alerts and management tools to prevent, detect, and remediate security threats, enabling admins to act immediately if an incident occurs.

[Chrome Education Upgrade](#) centralizes Chromebook fleet management and unlocks the full capabilities of ChromeOS, including access controls and advanced built-in security for Chrome devices.

## How do Google products protect younger students?

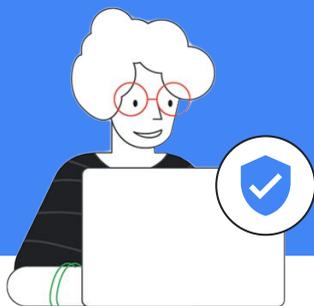
Built-in default settings protect students designated as under the age of 18. Admins can prevent or allow access to some services based on age at the district, school, class, and individual student levels. For example, schools can restrict YouTube content and enable [SafeSearch](#) and Safe Sites to screen out inappropriate results, preventing students from viewing unsafe websites.

Digital safety standards also apply to third-party EdTech apps and extensions that are featured in the Google for Education App Hub. Google for Education enables admins with application access control badges, App Licensing, and context-aware access rules for scalable control and visibility.

## How can parents or guardians help their children be safer online?

Enterprise-grade privacy and security are built in to the very foundation of Google for Education. For guardians and families, we also offer a range of resources to help understand and secure their child's digital learning environment, including our:

- [Guardian's Guide to Privacy & Security](#): An overview of how Google for Education tools interact to provide safer learning
- [Be Internet Awesome Family Guide](#): Includes resources to learn about online safety and digital citizenship at home
- [Tech Toolkit for Families and Guardians](#): A brief video explaining how Google for Education protects security with built-in protections
- [Digital Wellbeing Family Guide](#): Conversation starters for tough tech questions and help navigating the digital world as a family
- [Family Link](#): An app that enables guardians to set screen time, find quality content, and build healthy digital habits
- [Family Safety Center](#): Expert and educator tips for managing technology for your family
- [Families.google](#): Resource hub for raising digitally responsible children



Google for Education

© 2023 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043.



Review more about safer learning environments with Google for Education